17. (Twice Amended) A method according to claim 9, wherein said access status data is stored in a data store of at least one of said resource servers.

REMARKS

Reconsideration and allowance of this application are respectfully requested. Currently, claims 1-19 are pending in this application.

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached is captioned "**Version With Markings to Show Changes Made**."

Rejections Under 35 U.S.C. §102 and §103:

Claims 1, 3, 4, 8-11, 13 and 15-19 were rejected under 35 U.S.C. §102(e) as allegedly being unpatentable over Levergood et al (U.S. '780, hereinafter "Levergood"). Applicant respectfully traverses this rejection.

For a reference to anticipate a claim, each element must be found, either expressly or under principles of inherency, in the reference. Applicant respectfully submits that Levergood fails to disclose (or even suggest) each element of the claimed invention. For example, Levergood fails to disclose the following limitations of independent claim 1:

> "storing at the resource server:
> (1) an identifier for the client terminal, the identifier indicating said terminal to be a currently authenticated terminal; and
> (2) the access status of the user of the currently authenticated terminal; and
>
> enabling said resource server to validate a request for said document from the client terminal of said user, which request includes

said identifier, by checking that said stored access status includes said document."

Similar comments apply to independent claim 9.

An exemplary embodiment of the claimed invention therefore (i) stores access status data and an identifier indicating a currently authenticated terminal at the resource server, and (ii) validates document requests by a resource server by checking the access status data stored at the resource server. The claimed method therefore involves the check of something other than the identifier for validity. In particular, the associated access status data is checked.

Levergood discloses an authentication server 54 which performs the authentication of a client terminal 50 and then issues a command (the re-direct command) to re-direct the client terminal 50 to a desired content server 52. The re-direct command provides a URL which, in addition to the normal URL of the content server 52, also includes what is referred to as a session identification (SID). (See step 9 in Fig. 3 of Levergood.) Content server 52 may validate the URL/SID when it receives a command from the client terminal 50 for documents.

The system described in Levergood does not store access status data in a resource server, the status data indicating that an identifier is a validated identifier (of a terminal of a currently authenticated user). Levergood refers to a SID with which contains status data. However, Levergood specifies that the status data is stored on the client terminal. Levergood thus fails to disclose storing access data in the resource server.

Accordingly, Applicant respectfully submits that claims 1, 3, 4, 8-11, 13 and 15-19 are not anticipated by Levergood and respectfully requests that the rejection of these claims under 35 U.S.C. §102 be withdrawn.

Claim 2 was rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood in view of Kirsch (U.S. '915). Claims 5-7, 12 and 14 were rejected under 35 U.S.C. §103 as allegedly being unpatentable over Levergood in view of See et al (U.S. '243, hereinafter "See"). Applicant respectfully traverses these rejections.

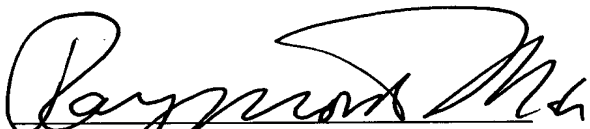
Since claims 2, 5-7, 12 and 14 depend from one of independent claims 1 and 9, all of the comments made above with respect to Levergood apply equally to these claims. Neither Kirsch nor See remedies the above deficiencies of Levergood discussed above with respect to the claimed invention. Accordingly, even if Kirsch or See were combined with Levergood, the resulting combinations would not have taught or suggested all of the claimed limitations. Accordingly, Applicant respectfully requests that the rejections of claims 2, 5-7, 12 and 14 under 35 U.S.C. §103 be withdrawn.

Conclusion:

Applicant believes that this entire application is in condition for allowance and respectfully requests a notice to this effect. If the Examiner has any questions or believes that an interview would further prosecution of this application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Raymond Y. Mah
Reg. No. 41,426

RYM/sl
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703)816-4044
Facsimile: (703)816-4100

VERSION WITH MARKINGS TO SHOW CHANGES MADE IN THE CLAIMS:

1. (Twice Amended) A method of operating an authenticating server system for authenticating users at client terminals connected via a data communications network, to control access to [a] documents stored on a resource server, said method comprising performing the following in said server system:

storing in the resource server authentication details and access status data of authorized users;

receiving at the resource server authentication data for a user from a client terminal of the user and validating at the resource server said authentication data by reference to said stored authentication details;

storing at the resource server:

[issuing] (1) an identifier for the [user's] client terminal, [to said terminal for storage thereon,] the identifier [being transmitted in such a manner that the identifier is retransmitted by said user's client terminal with document requests directed at said resource server;] indicating said terminal to be a currently authenticated terminal; and

[storing status data indicating said identifier to be a validated identifier of a terminal of a currently authenticated user, in response to the receipt and validation of the authentication data; and]

(2) the access status of the user of the currently authenticated terminal; and

enabling said resource server to validate a request for said document from the [user's] client terminal of said user, which request includes said identifier, by checking that said [status data] stored access status includes said document [on receipt of said document request].

2. (Twice Amended) A method according to claim 1, wherein said identifier is transmitted in a cookie to said [user's] client terminal.

3. (Thrice Amended) A method according to claim 1, wherein said identifier is received from said [user's] client terminal with said authentication data.

4. (Twice Amended) A method according to claim 3, wherein a new identifier is issued to said [user's] client terminal if said authentication data is invalid.

5. (Twice Amended) A method according to claim 4, wherein said identifier comprises data indicating the number of times an invalid authenticator has been received from said [user's] client terminal.

6. (Twice Amended) A method according to claim 5, wherein said method comprises issuing no further identifier to said [user's] client terminal if an identifier received from said [user's] client terminal indicates that a

predetermined number of invalid authenticators have been received from said [user's] client terminal.

7. (Thrice Amended) A method according to claim 1, comprising timing out said identifier as an identifier of a terminal of a currently authenticated user if no document request is received from said [user's] client terminal for a predetermined period.

8. (Thrice Amended) A method according to claim 1, comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain; and

enabling each of said Web servers to validate document requests from the [user's] client terminal, which requests include said identifier, by checking said status data on receipt of a document request.

9. (Twice Amended) A method of operating an authenticating server system for authenticating users at client terminals remotely connected via a data communications network, to control access to a plurality of resource servers, said method comprising performing the following steps in said server system:

storing in at least one of the resource servers authentication details and access status data of authorized users;

performing at the at least one of the resource servers remote authentication of a user by reference to said stored authentication details and during said remote authentication step generating the access status data of the user, distinguishing said user from other users which are not currently authenticated, and a secret encryption key shared with said user;

storing said access status data in [storage means accessible to said plurality of] the at least one of the resource servers to check an authentication status of said user by using an identifier for the [user's] client terminal received in a service request to check the stored access status data; and

storing said shared secret key in a data store accessible by at least one of said resource servers for use during communications with said user.

10. (Twice Amended) A method according to claim 9, wherein said remote authenticating step comprises issuing a challenge to the [user's] client terminal, receiving a response to said challenge, and verifying said response.

11. (Twice Amended) A method according to claim 9, further comprising updating said access status data for an authenticated user following said storing step.

12. (Amended) A method according to claim 11, wherein said updating step is performed in response to a time-out associated with said access status data.

13. (Amended) A method according to claim 11, wherein said updating step is performed in response to access by one of said resource servers to said access status data.

14. (Thrice Amended) A method according to claim 12, wherein said updating step is performed in response to a request by the [user's] client terminal.

15. (Thrice Amended) A method according to claim 9, wherein said identifier is an IP address of the [user's] client terminal.

16. (Thrice Amended) A method according to claim 9, wherein said authentication step comprises issuing said identifier to the [user's] client terminal.

17. (Twice Amended) A method according to claim 9, wherein said access status data is stored in a data store of at least one of [which] said resource servers [are each able to access].